LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-450494

LL-08 Electronic Data Storage Devices100818

C. DeGrange

August 20, 2010

Disclaimer

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

Contractor Assurance Office

Lessons Learned

LL-2010-LLNL-08
LLNL-AR-XX
August 20, 2010

Security Problems Can Arise if Responsibilities for Electronic Data Storage Devices Are Not Met

To ensure that information security requirements are met, line managers and custodians of electronic data storage devices need to be aware of and compliant with their responsibilities.

A property inventory conducted in April could not locate a computer-connected personal digital assistant (PDA) and it was reported lost. Because it was believed to contain the birth dates (personally identifiable information) of more than ten individuals, the loss was reported to the Department of Energy (DOE) headquarters within an hour of discovery as an Impact Measurement Index 1 (IMI-1) security incident. According to the DOE, IMI-1incidents represent the highest level of security concern. They are “actions, inactions, or events that pose the most serious threats to national security interests and/or critical assets.”

The PDA was later found in the custodian’s car. A subsequent review determined that it did not contain sensitive information and the incident was rescinded. Although rescinded, the conditions associated with the incident indicate possible significant security incidents if not corrected.

Analysis

1) LLNL has thousands of computer-connected electronic data storage devices. Examples include disk drives (internal or external to computers), CDs, DVDs, memory sticks, magnetic tapes, recording equipment (audio, video/cameras, optical, or data), and items with a data exchange port that can be connected to a computer system (e.g., BlackBerries, PDAs, cellular telephones, smart phones, etc.).
2) These devices come with specific custodial responsibilities. Some of these responsibilities result from the information contained on the device. For example, Unclassified Controlled Information (UCI), taken offsite must be encrypted. In some cases, that means full disk encryption. In cases where full disk encryption is not possible, the sensitive unclassified data itself must be encrypted. Other responsibilities arise because a device’s features present a security risk that must be controlled. For example, cellular telephones, smart phones and BlackBerries have restrictions governing where they are allowed, which functionalities are allowed to remain active, and which functionalities are allowed to be used in certain locations.
3) In the instance discussed above, the custodian forgot where the PDA was stored after a period of non-use.
4) The custodian did not excess the PDA because management had not evaluated and communicated the risks and likely consequences associated with its retention.
5) Without such an evaluation, management placed no emphasis on monitoring employee performance to property return tasks specified as requirements in Laboratory property management processes.

Recommended Action

These actions apply to all electronic data storage devices, regardless of whether they are individually tracked in an LLNL inventory system.

Management:

1) When technology changes, as it has with smart phones supplanting cellular telephones and computer-connected PDAs, assess and communicate the liabilities that result from retention of the outdated technology.
2) When standards change, as they have with a new requirement for full disk encryption of laptop computers and the use of approved encryption of UCI on memory storage devices taken off Department of Energy sites, assess and communicate the liabilities that result from the retention of the non-compliant technology.
3) Once the risks are determined, balance business needs against risks and make explicit decisions about what property items to keep or excess.
4) Monitor returns of property with security liabilities and emphasize an accelerated return process.
5) If property with security liabilities will continue in service, consider additional controls to reduce the risks associated with continued use of the property.
6) On an annual basis, supervisors should assess the needs of their workforce to determine communication needs and to ensure encryption is used as required to protect UCI. Supervisors must ensure employees use encryption on electronic data storage devices to protect UCI when taken off site. In addition, supervisors should facilitate the use of file encryption to protect information stored on backup media and computer files which stay on site.

Custodians:

1) Conduct a personal inventory of all Laboratory-issued electronic data storage devices in your possession, including those not currently in use or tracked by an LLNL inventory system.
2) For each device, know the types and categories of information stored on it and the current custodian requirements. Ensure that you are in compliance even if the device is no longer in use. Note that standards may have changed since the device was put into service (e.g., encryption of sensitive unclassified information is required for all devices removed from Department of Energy sites, even if the device was put into service before this requirement took effect).
3) If a device is no longer in use or needed elsewhere within your organization, promptly return it to Property Management through your Directorate Property Center for disposal.

Where to Get Help or More Information

- Your supervisor.
- Your Directorate Security Officer (DSO): https://security-r.llnl.gov/directorateContacts.shtml
- Your Organizational Information System Security Officer (OISSO): https://www-csp.llnl.gov/oisso/oisso.html
- Security Organization Contacts: https://security-r.llnl.gov/serviceHours.shtml
- Integrated Safeguards & Security Management: https://security-r.llnl.gov/issm/issm.shtml
- LLNL's cell phone administrator, 3-1815 (BlackBerry devices, cell phones and Smartphones). Also reference https://pao-int.llnl.gov/news/2010/aug/docs/081010_blackberry.php.

- PII discussion: https://uci-r.llnl.gov/pii/pii.html
- Link to Directorate Property Center contacts: https://property-int.llnl.gov/contacts.html
- Policy regarding the use of encryption on mobile devices and removable media: https://www-csp.llnl.gov/pubs/u-docs/P2029.pdf
- Procedure for disposal of government property: https://property-int.llnl.gov/policies.html. Click on the Policies & Procedures tab, click on Excess Procedure in the drop-down menu.
- Procedure for destruction of equipment containing electronic storage media: https://property-int.llnl.gov/policies.html. Click on the Policies & Procedures tab, click on Excess Procedure in the drop-down menu.
- To search for other LLNL Lessons Learned, go to the "Lessons Learned" Web site (https://ll.llnl.gov) and select the topic of interest or click on "Search" and enter a keyword.

Keywords: electronic data storage, personal data assistant, PDA, personal organizer

ISSM Functions: analyze the hazard, develop and implement controls, perform work to the control

Search Category: BlackBerry, cell phone, computer connected, electronic data storage, information security, personal digital assistant, PDA, personally identifiable information, PII, Smartphone.

Please Post

LessonsLearned@llnl.gov